

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-003432

(43)Date of publication of application : 06.01.1998

(51)Int.Cl. G06F 12/14
G06F 3/06
G11B 7/00
G11B 20/10

(21)Application number : 08-157816

(71)Applicant : NEC CORP

(22)Date of filing : 19.06.1996

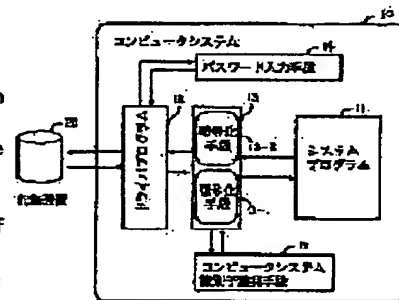
(72)Inventor : SATO YASUSHI

(54) DATA RECORDING AND REPRODUCING SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a data recording/reproducing system which can improve the secrecy of data without executing the processing of remodeling, extension and substitution on a recording device and a medium itself, which are operated at present.

SOLUTION: The system is applied to a computer system 10 to which the recording device 20 recording and reproducing data into/from the recording medium. At the time of recording and reproducing data into/from the recording medium by the recording device 20, a password corresponding to the recording device 20 itself is combined with identification information of the computer system 10 itself and they are used. Then, data is ciphered and decoded.



LEGAL STATUS

[Date of request for examination] 19.06.1996

[Date of sending the examiner's decision of rejection] 12.07.2000

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection] 2000-12702

[Date of requesting appeal against examiner's decision of rejection] 10.08.2000

BEST AVAILABLE COPY

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-3432

(43) 公開日 平成10年(1998) 1月6日

(51) Int. Cl. ⁹	識別記号	序内整理番号	F 1	技術表示箇所
G 0 6 F 12/14	3 2 0		G 0 6 F 12/14	3 2 0 B
	3 0 4			3 0 4 H
G 1 1 B 7/00		9484-5D	G 1 1 B 7/00	R
20/10		7736-5D	20/10	H

審査請求 有 請求項の数 3 O L (全 8 頁)

(21) 出願番号 特願平8-157816

(22) 出願日 平成8年(1996) 6月19日

(71) 出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72) 発明者 佐藤 靖士

東京都港区芝五丁目7番1号 日本電気株式会社内

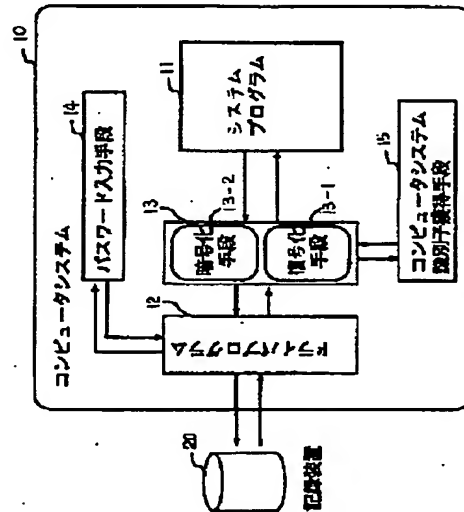
(74) 代理人 弁理士 後藤 祥介 (外2名)

(54) 【発明の名称】 データ記録再生方式

(57) 【要約】

【課題】 現在運用している記録装置や媒体自体に改造、増設、置換等の処置を行わずとも、データの機密性を向上できるデータ記録再生方式を提供する。

【解決手段】 記録媒体に対してデータの記録、再生を行う記録装置20が接続されるコンピュータシステム10に適用される。記録装置20による記録媒体へのデータの記録、再生に際して、記録装置20自体に対応するパスワードとコンピュータシステム10自体の識別情報とを組み合わせて用いて、データの暗号化、復号化を行う。



(2)

特開平10-3432

【特許請求の範囲】

【請求項1】 各種記録媒体に対してデータの記録、再生を行う各種記録装置が接続されるコンピュータシステムに適用され、記録装置による記録媒体へのデータの記録、再生に際して、記録装置個々にそれぞれ対応するパスワードとコンピュータシステム自体の識別情報とを組み合わせ用いてデータの暗号化、復号化を行うことを特徴とするデータ記録再生方式。

【請求項2】 前記コンピュータシステムは、記録装置の制御を行うと共に、前記パスワードを保存するドライバプログラムと、前記ドライバプログラムに接続され、記録装置個々の前記パスワードを入力するためのパスワード入力手段と、前記ドライバプログラムに接続され、記録装置による記録媒体へのデータの記録、再生に際して、データの暗号化、復号化を行う暗復号化手段と、前記暗復号化手段に接続され、コンピュータシステム自体の識別情報を獲得する識別情報獲得手段とを有することを特徴とする請求項1に記載のデータ記録再生方式。

【請求項3】 前記コンピュータシステムは、記録装置の制御を行うと共に、前記パスワードを保存するドライバプログラムと、前記ドライバプログラムに接続され、記録装置個々の前記パスワードを入力するためのパスワード入力手段と、前記ドライバプログラムに接続され、記録装置による記録媒体へのデータの記録、再生に際して、データの暗号化、復号化を行う暗復号化手段と、前記暗復号化手段に接続され、コンピュータシステム自体の識別情報を獲得する識別情報獲得手段とを仮想ドライバプログラムとして有することを特徴とする請求項1に記載のデータ記録再生方式。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、各種記録装置が接続されるコンピュータシステムに適用されるデータ記録再生方式に関する。

【0002】

【従来の技術】 従来、この種のデータ記録再生方式においては、記録されたデータが第三者によって不正な閲覧がされることを防止するためにデータの暗号化が用いられることが多い。

【0003】 従来のデータ記録再生方式は、例えば、特開平6-274880号公報に記載されている。この公報に記載されたデータ記録再生方式は、情報記録媒体上に暗号化のための特別な領域を設定し、暗号化手段をそこに記録する方式である。情報記録媒体上には、書換え可能なデータ記録領域と読出し専用のデータ記憶領域とを設定する。そして、データ記録領域に書き込むデータの暗号化を行う読出し専用の記憶領域に格納された暗号化プログラムと、同じく読出し専用の記憶領域に格納された暗号化されたデータの解読を行う復号化プログラムとを含んでいる。

【0004】 このデータ記録再生方式において、情報記録媒体へ情報を記録する際には、まず、媒体上の読み出し専用の記憶領域に記録された暗号化プログラムを読み込み、暗号化のための暗号キーを使用してデータを暗号化し、媒体上に記録する。一方、情報記録媒体からのデータの参照の際には、媒体上の読み出し専用の記憶領域に記録された復号化プログラムを読み込み、上記暗号キーを使用して、媒体上のデータを再生する。

【0005】 従来のデータ記録再生方式の他の一例が、特開平4-98552号公報に記載されている。この公報に記載されたデータ記録再生方式は、外部記録装置とデータをアクセスするファイリング装置との間に、暗号化手段および復号化手段が着脱可能となる回路を設けている。そして、着脱可能な暗号化および復号化手段を、データをアクセスするファイリング装置と別の所に保管することで、不正なデータのアクセスを防止する方式である。このシステムにおいては、データを作成または閲覧するデータ処理手段と、作成されたデジタルデータを記憶する外部記録装置と、記憶するデータを暗号化する取り外し可能な暗号化手段と、暗号化されたデータを復元する取り外し可能な復号化手段とを含んでいる。データの記録の際には、暗号化手段を用いて暗号化し、外部記録装置に記録する。一方、データの参照の際には、復号化手段によって外部記録装置に記録されているデータを復元し、参照する。また、暗号化手段または復号化手段の少くとも一方を取り外すことにより、データへのアクセスを制限している。

【0006】

【発明が解決しようとする課題】 上述した例をも含め、従来のデータ記録再生方式においては、暗号化のための専用の媒体または回路を必要とするため、使用する記録装置が限定されたり、特殊な暗号化装置を装備したハードウェアを用いる必要がある。

【0007】 また、媒体上の書き込み不可の領域に、暗号化プログラムが組み込まれている場合には、この暗号化プログラムに問題があると、媒体の再利用が不可能となるため、全ての媒体を書き換えなければならなくなる。

【0008】 さらに、記録媒体上の特定のデータの内容が判明している場合には、媒体上の暗号化プログラムを解析することにより、暗号化されたデータと予め判明しているデータとを照合することで、パスワードが類推される虞がある。

【0009】 本発明の課題は、現在運用している記録装置や媒体自体に改訂、増設、置換等の処置を行わずとも、データの機密性を向上できるデータ記録再生方式を提供することである。

【0010】 本発明の他の課題は、データを暗号化して保存する際に、特定の種類の記録装置、媒体に限定せず、あらゆる記録装置を使用することを可能にしたデー

3

タ記録再生方式を提供することである。

【0011】本発明のさらに他の課題は、記録媒体上に、データの暗号化手段となるプログラムやアクセス制限のためのキーワード等を設けることや、暗号作成用のパスワードをコンピュータシステム上のファイル等に保存することが必要がなく、暗号化の解析が困難なデータ記録再生方式を提供することである。

【0012】

【課題を解決するための手段】本発明によれば、各種記録媒体に対してデータの記録、再生を行う各種記録装置が接続されるコンピュータシステムに適用され、記録装置による記録媒体へのデータの記録、再生に際して、記録装置個々にそれぞれ対応するパスワードとコンピュータシステム自体の識別情報とを組み合わせて用いてデータの暗号化、復号化を行うことを特徴とするデータ記録再生方式が得られる。

【0013】本発明によればまた、前記コンピュータシステムは、記録装置の制御を行うと共に、前記パスワードを保存するドライバプログラムと、前記ドライバプログラムに接続され、記録装置個々の前記パスワードを入力するためのパスワード入力手段と、前記ドライバプログラムに接続され、記録装置による記録媒体へのデータの記録、再生に際して、データの暗号化、復号化を行う暗号化手段と、前記暗号化手段に接続され、コンピュータシステム自体の識別情報を獲得する識別情報獲得手段とを有することを特徴とする前記データ記録再生方式が得られる。

【0014】本発明によればさらに、前記コンピュータシステムは、記録装置の制御を行うと共に、前記パスワードを保存するドライバプログラムと、前記ドライバプログラムに接続され、記録装置個々の前記パスワードを入力するためのパスワード入力手段と、前記ドライバプログラムに接続され、記録装置による記録媒体へのデータの記録、再生に際して、データの暗号化、復号化を行う暗号化手段と、前記暗号化手段に接続され、コンピュータシステム自体の識別情報を獲得する識別情報獲得手段とを有することを特徴とする前記データ記録再生方式が得られる。

【0015】

【発明の実施の形態】以下、図面を参照して、本発明の実施の形態によるデータ記録再生方式を説明する。

【0016】【実施の形態1】図1は、本発明の実施の形態1によるデータ記録再生方式を実現する構成を示すブロック図である。

【0017】図1を参照して、本データ記録再生方式は、各種記録媒体に対してデータの記録、再生を行う各種記録装置の一例として記録装置20が接続されるコンピュータシステム10に適用される。記録装置20による記録媒体へのデータの記録、再生に際して、記録装置20に対応するパスワードとコンピュータシステム10

(3)

特開平10-3432

4

自体の識別情報（コンピュータシステム識別子）とを組み合わせて用いてデータの暗号化、復号化を行うものである。そして、コンピュータシステム10は、記録装置20の制御を行うと共に、パスワードを保存するドライバプログラム12と、ドライバプログラム12に接続され、記録装置20（ならびに記録装置20以外の記録装置）のパスワードを入力するためのパスワード入力手段14と、ドライバプログラム12に接続され、記録装置20による記録媒体へのデータの記録、再生に際して、データの暗号化、復号化を行う暗号化手段13と、暗号化手段13に接続され、コンピュータシステム10自体のコンピュータシステム識別子を獲得するコンピュータシステム識別子獲得手段15とを有している。暗号化手段13は、復号化手段13-1と、暗号化手段13-2とを含んでいる。

【0018】ドライバプログラム12以外のシステムの動作を司るシステムプログラム11は、記録媒体上のデータの記録に、暗号化手段13-2を使用する。暗号化手段13-2は、記録装置20を制御、管理するドライバプログラム12（以下、単にドライバプログラム12と呼ぶ）から、データを記録する記録装置20に対するパスワードを獲得し、コンピュータシステム識別子獲得手段15を使用してコンピュータシステム識別子を獲得する。暗号化手段13-2はまた、獲得したパスワードとコンピュータシステム識別子を使用してデータの暗号化を行う。ドライバプログラム12は、記録装置20が、コンピュータシステム起動後に一度もデータの参照（データの記録または再生）をしていない場合か、あるいは記録装置20またはその記録媒体が交換に一度も参照されていない場合には、暗号化手段13-2に渡すパスワードをパスワード入力手段15を使用して獲得する。ドライバプログラム12はまた、記録装置20がコンピュータシステム10の起動後少くとも一回以上参照されており、記録装置20の参照後に記録装置20の交換またはその記録媒体の交換が行われておらず、さらに記録装置20の参照後にコンピュータシステム10が停止していない場合には、それ以前の参照の際にパスワード入力手段15を使用して獲得したパスワードを暗号化手段13-2に渡す。暗号化手段13-2は、ドライバプログラム12から獲得したパスワードと、コンピュータシステム識別子獲得手段15を使用して獲得したコンピュータシステム識別子とを使用して、データの暗号化を行う。ドライバプログラム12はさらに、暗号化手段13-2によって暗号化したデータを記録媒体に記録装置20によって記録する。

【0019】他方、システムプログラム11は、記録装置20上のデータの再生（読み出し）に、復号化手段13-1を使用する。復号化手段13-1は、ドライバプログラム12から、記録装置20に対するパスワードを獲得し、コンピュータシステム識別子獲得手段15を使

(4)

特開平10-3432

5

用してコンピュータシステム識別子を獲得する。ドライバプログラム12は、記録装置20が、コンピュータシステム起動後に一度も参照されていない場合か、あるいは記録装置20またはその記録媒体が交換後に一度も参照されていない場合には、復号化手段13-1に渡すパスワードを、パスワード入力手段15を使用して獲得する。ドライバプログラム12は、記録装置20がコンピュータシステムの起動後に少なくとも一回以上参照されており、記録装置20参照後に記録装置20の交換またはその記録媒体の交換が行われておらず、さらに記録装置20の参照後にコンピュータシステムが停止していない場合には、それ以前の参照の際にパスワード入力手段15を使用して獲得したパスワードを復号化手段13-1に渡す。復号化手段13-1は、ドライバプログラム12を使用し、記録媒体上の暗号化されたデータを獲得する。復号化手段13-1は、獲得したパスワードとコンピュータシステム識別子とを使用して、ドライバプログラム12から獲得した暗号化されたデータの復号化を行う。

【0020】【実施の形態2】図2は、本発明の実施の形態2によるデータ記録再生方式を実現する構成を示すブロック図である。

【0021】図2を参照して、本データ記録再生方式は、実施の形態1と同様に、各種記録媒体に対してデータの記録、再生を行う各種記録装置の一例として外部記憶装置220と、ユーザプログラム230とが接続されるオペレーティングシステム210に適用される。外部記憶装置220は、固定ディスク装置220aと、テープドライブ220bとを有している。ユーザプログラム230は、固定ディスク装置220aを直接使用する第1のプログラム231と、ファイルシステムプログラム211を使用してディスクドライバを使用する第2のプログラム232と、ファイルシステムプログラム211を使用して後述する仮想ディスクドライバを使用する第3のプログラム233と、仮想ディスクドライバを直接使用する第4のプログラム234と、テープドライブを使用する第5のプログラム235と、仮想テープドライブを使用する第6のプログラム236とを含んでいる。そして、外部記憶装置220による記録媒体へのデータの記録、再生に際して、外部記憶装置220に対応するパスワードとオペレーティングシステム210自体の識別情報（コンピュータシステム識別子）とを組み合わせて用いてデータの暗号化、復号化を行うものである。

【0022】固定ディスク装置220aは、ファイルシステムプログラム211で管理された第1領域220a-1と、ファイルシステムプログラムで管理されていない第2領域220a-2とを含んでいる。

【0023】また、オペレーティングシステム210は、外部記憶装置220の制御を行うと共に、パスワ

6

ドを保存するドライバプログラムとして、固定ディスク装置用の仮想ドライバプログラム60aと、テープドライブ用の仮想ドライバプログラム60bとを有している。仮想ドライバプログラム60a（60b）の構成を図3に示す。

【0024】図2および図3を参照して、仮想ドライバプログラム60a（60b）は、外部記憶装置220（固定ディスク装置220a、テープドライブ220b）の制御を行うと共に、パスワードを保存するドライバプログラム62a（62b）と、ドライバプログラム62a（62b）に接続され、外部記憶装置220（ならびに外部記憶装置220以外の記録装置）のパスワードを入力するためのパスワード入力手段64と、ドライバプログラム62a（62b）に接続され、外部記憶装置220による記録媒体へのデータの記録、再生に際して、データの暗号化、復号化を行う暗復号化手段63と、暗復号化手段63に接続され、オペレーティングシステム210自体のコンピュータシステム識別子を獲得するコンピュータシステム識別子獲得手段15とを有している。仮想ドライバプログラム60a（60b）は、使用するドライバプログラム62a（62b）と同一の外部インターフェースを持っている。暗復号化手段63は、復号化手段63-1と、暗号化手段63-2とを含んでいる。

【0025】次に、図2および図3を参照して、本方式の動作について説明する。

【0026】第3のプログラム233は、固定ディスク装置220aの第1領域220a-1（参照領域）のデータを参照するために、ファイルシステムプログラム211を使用する。ファイルシステムプログラム211は、ユーザプログラム230からのデータの参照要求に対応する参照領域を参照するために、固定ディスク装置用のドライバプログラム62aを呼び出す。仮想ドライバプログラム60aは、データの暗号化および復号化に必要なパスワードを暗復号化手段63を使用して固定ディスク装置用のドライバプログラム62aに要求する（C1）。パスワードの要求を受けたドライバプログラム62aは、固定ディスク装置220aが、オペレーティングシステム210の起動後に参照されており、パスワードが既に獲得済みで、なおかつ固定ディスクがパスワード獲得後、オペレーティングシステム210から切り離されていない場合に、獲得済みのパスワードを暗復号化手段63へ渡す（R1）。固定ディスク装置220aが、オペレーティングシステム210起動後に一度も参照されていない場合、あるいは参照された後にオペレーティングシステム210から切り離されていた場合には、パスワード入力手段64にパスワードを要求する（C2）。パスワード入力手段64は、第3のプログラム233を使用するユーザーに対してパスワードを要求し、得られたパスワードを固定ディスク装置用のドライ

(5)

特開平10-3432

7

バプログラム62aに渡す(R2)。尚、パスワードの要求方法は、キーボードで入力させる方法や、フレキシブルディスク等に記録して読み出す方法等が例として考えられるが、これらに限定されるものではない。パスワード入力手段64からパスワードを獲得したドライバプログラム62aは、獲得したパスワードをメモリ上に保存し、暗復号化手段63へ渡す(R1)。暗復号化手段63は、コンピュータシステム識別子獲得手段65に、本オペレーティングシステム210を一意に決定するコンピュータシステム識別子(以後、一部を除いてホストコードと呼ぶ)を要求し(C3)、獲得する(R3)。

【0027】第3のプログラム233の参照が、記録(書き込み参照)であった場合には、仮想ドライバプログラム60aは、ファイルシステムプログラム211から参照領域に記録するデータを受け取り、暗復号化手段63に渡す。暗復号化手段63は、R1で獲得したパスワードと、R3で獲得したホストコードと、参照領域に記録するデータとを、暗号化手段63-2に渡す。暗号化手段63-2は、暗復号化手段63が獲得したパスワードとホストコードとを使用して、記録するデータを暗号化する。本発明では、暗号化の方法は、パスワードとホストコードとの異なる組合せで同一の暗号化が行われるパターンが発生しないような方法で、かつその方法が容易には類推できず、さらにデータが復号化可能な暗号化であることが必要である。暗復号化手段63は、暗号化されたデータと、固定ディスクの参照領域にデータを書き込む命令とを、ドライバプログラム62aに渡す(DW1)。ドライバプログラム62aは、参照領域にデータを書き込む。

【0028】一方、第3のプログラム233の参照が、再生(読み出し参照)であった場合には、暗復号化手段63は、ドライバプログラム62aに参照領域のデータを読み出す命令を渡す(DW1)。ドライバプログラム62aは、DW1をもとに参照領域のデータを読み出し、暗復号化手段63に渡す(DR1)。暗復号化手段63は、R1で獲得したパスワードと、R3で獲得したホストコードと、復号化するデータとを、復号化手段63-1に渡す。復号化手段63-1は、獲得したパスワードとホストコードとを使用してデータを復号化する。仮想ドライバプログラム60aは、暗復号化手段63にて復号したデータをファイルシステムプログラム211に渡す。ファイルシステムプログラム211は、参照領域から仮想ドライバプログラム60aを使用して再生したデータを第3のプログラム233に渡す。

【0029】以上の動作により、第3のプログラム233は、固定ディスク装置220a(の固定ディスク)上の参照領域のデータを参照する。

【0030】上記動作例において、第3のプログラム233は、データの暗号化を全く意識することなく、通常のファイルシステム211上にあるファイルを扱う例え

8

ば第2のプログラム231と同様の操作によってデータを暗号化し、記録することが可能となる。

【0031】また、上記動作例において、パスワードはオペレーティングシステム210が装置を最初に認識した時点、あるいは装置内の媒体を最初に認識した時点で入力を行うが、これに加えて任意の時点でパスワードの変更を可能にして運用することも可能である。

【0032】さて、上記動作例では、第3のプログラム233はファイルシステムプログラム211を使用し、固定ディスク装置220a上のデータの参照を行った。しかしながら、本実施の形態では、ファイルシステムプログラムを使用しない装置、あるいはファイルシステムを構築できない記録装置(テープドライブ220b)に対しても、暗号化を行う参照が可能である。以下にその動作例を示す。

【0033】第6のプログラム236は、テープドライブ220b内のテープ媒体のデータを参照するために、テープドライブ用の仮想ドライバプログラム60bを使用する。仮想ドライバプログラム60bは、データの暗号化および復号化に必要なパスワードを暗復号化手段63を使用してテープドライブ用のドライバプログラム62bに要求する(C1)。パスワードの要求を受けたドライバプログラム62bは、テープドライブ220bが、オペレーティングシステム210の起動後に参照されており、パスワードが既に獲得済みで、なおかつテープドライブ220b内のテープ媒体がパスワード獲得後取り出されていない場合には、獲得済みのパスワードを暗復号化手段63へ渡す(R1)。テープドライブ220bが、オペレーティングシステム210の起動後に一度も参照されていない場合か、あるいは参照された後にテープ媒体がテープドライブ220bから取り出されていた場合には、パスワード入力手段64にパスワードを要求する(C2)。パスワード入力手段64は、第3のプログラム233を使用するユーザーにパスワードを要求し、得られたパスワードをドライバプログラム62bに渡す(R2)。パスワード入力手段64からパスワードを獲得したドライバプログラム62bは、獲得したパスワードをメモリ上に保存し、暗復号化手段63へ渡す(R1)。暗復号化手段63は、コンピュータシステム識別子獲得手段65に、オペレーティングシステム210を一意に決定するホストコードを要求し(C3)、獲得する(R3)。

【0034】第6のプログラム236の参照が、記録(書き込み参照)であった場合には、仮想ドライバプログラム60bは、第6のプログラム236から記録するデータを受け取り、暗復号化手段63に渡す。暗復号化手段63は、R1で獲得したパスワードと、R3で獲得したホストコードと、テープ媒体に記録するデータとを、暗号化手段63-2に渡す。暗号化手段63-2は、暗復号化手段63が獲得したパスワードとホストコ

(6)

特開平10-3432

9

ードとを使用して、記録するデータを暗号化する。暗号化手段63は、暗号化されたデータと、データをテープ媒体に書き込む命令とを、ドライバプログラム62bに渡す(DW1)。ドライバプログラム62bは、テープドライブ220bにデータ(DW1)を書き込む。

【0035】一方、第6のプログラム236の参照が、再生(読み出し参照)であった場合には、暗号化手段63は、ドライバプログラム62bにテープドライブ220b内のテープ媒体上のデータを読み出す命令を渡す(DW1)。ドライバプログラム62bは、DW1をもとにテープ媒体上のデータを読み出し、暗号化手段63に渡す(DR1)。暗号化手段63は、R1で獲得したパスワードと、R3で獲得した干すとコードと、復号するデータとを、復号化手段63-1に渡す。復号化手段63-1は、獲得したパスワードとホストコードとを使用してデータを復号化する。仮想ドライバプログラム60bは、暗号化手段63で復号化したデータを第6のプログラム236に渡す。

【0036】以上の動作により、第6のプログラム236はテープドライブ220b内のテープ媒体上のデータを参照する。

【0037】上記動作例において、第6のプログラム236は、データの暗号化を全く意識することなく、通常のテープドライブ220b内のテープ媒体上にあるデータを扱う例えば第5のプログラム235と同様の操作によってデータを暗号化し、記録することが可能である。

【0038】尚、以上説明した実施の形態においては、記録装置として固定ディスク装置とテープドライブを例示して本発明によるデータ記録再生方式を説明したが、その他の光ディスク装置や、カードドライブ装置等、ドライバプログラム經由で参照されるあらゆる記録装置に対して、本発明は適用可能である。

【0039】

【発明の効果】本発明によるデータ記録再生方式は、各種記録媒体に対してデータの記録、再生を行う各種記録装置が接続されるコンピュータシステムに適用され、記録装置による記録媒体へのデータの記録、再生に際して、記録装置毎々にそれぞれ対応するパスワードとコンピュータシステム自体の識別情報とを組み合わせて用いてデータの暗号化、復号化を行うため、以下に示す効果を奏する。

【0040】第1の効果は、情報を記録する装置および媒体に、特殊な機構あるいは装置を追加することなく、従来使用していたディスク装置、テープドライブ、カードドライブ、光ディスク装置等のあらゆる記録媒体に対して、記録するデータの暗号化が可能となり、機密保持性の高い情報の記録、再生を実現することである。

【0041】第2の効果は、記録装置に記録された情報

10

には、記録したコンピュータシステムに依存した暗号化が施されるため、他のコンピュータシステム上ではデータを再生することが不可能となることである。したがって、不正に情報記録装置、あるいは媒体が持ち出されても、他のコンピュータシステム上に再生することが不可能であり、機密保持性の高い、情報の記録再生が実現できる。

【0042】第3の効果は、記録装置に記録するデータの暗号化を行わない記録と、暗号化を行う記録を共存させることが可能であり、さらに同一記録媒体に対してパスワードを複数使用すると、異なる暗号化を行ったデータの共存が可能となるため、重要なデータを分割し、異なるパスワードによってそれぞれを記録することで、一部のパスワードが破られても全体を参照することは極めて困難となり、機密保持性の高い情報の記録、再生を実現できることである。

【図面の簡単な説明】

【図1】本発明の実施の形態1によるデータ記録再生方式を実現する構成を示すブロック図である。

【図2】本発明の実施の形態2によるデータ記録再生方式を実現する構成を示すブロック図である。

【図3】図2に示す構成における仮想ドライバプログラムの詳細を示すブロック図である。

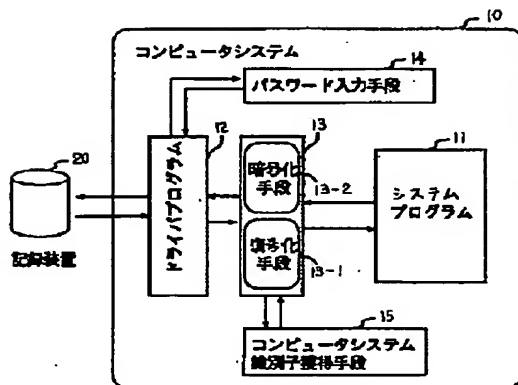
【符号の説明】

10 コンピュータシステム
11 システムプログラム
12 ドライバプログラム
13 暗号化手段
13-1 復号化手段
13-2 暗号化手段
14 パスワード入力手段
15 コンピュータシステム識別子獲得手段
20 記録装置
60a、60b 仮想ドライバプログラム
62a、62b ドライバプログラム
63 暗号化手段
63-1 復号化手段
63-2 暗号化手段
64 パスワード入力手段
65 コンピュータシステム識別子獲得手段
210 オペレーティングシステム
211 ファイルシステムプログラム
220 外部記憶装置
220a 固定ディスク装置
220b テープドライブ
230 ユーザープログラム
231~236 第1~第6のプログラム

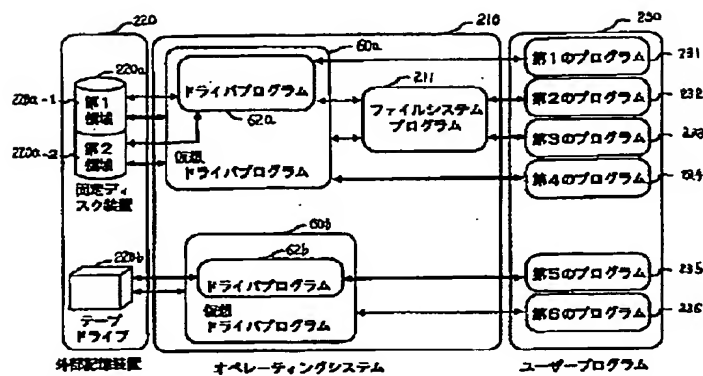
(7)

特開平10-3432

【図1】



【図2】



(8)

特開平10-3432

【図3】

